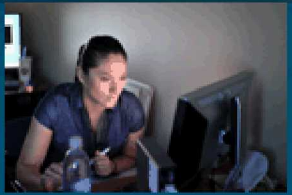
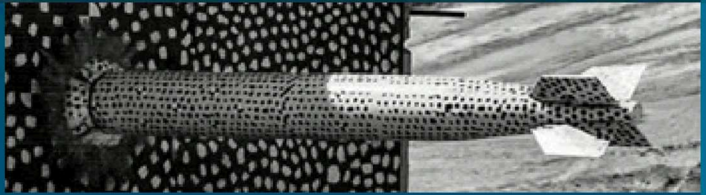
SAND2020-6706C

A Modular Approach to Trusted System Design for Arms Control Treaty Verification





PRESENTED BY

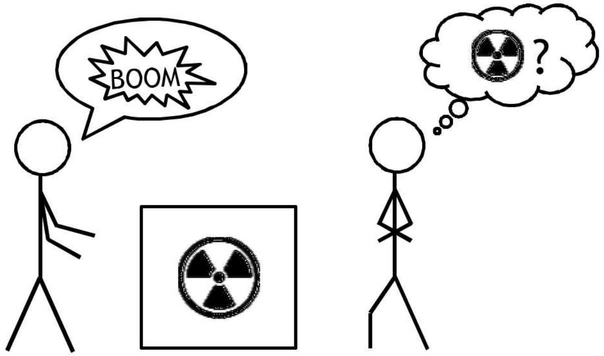
J. K. Polack, E. Brubaker, M. C. Hamel, R. R. Helguero, D. L. Maierhafer, P. Marleau, E. A. Padilla, T. M. Weber

13 July 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

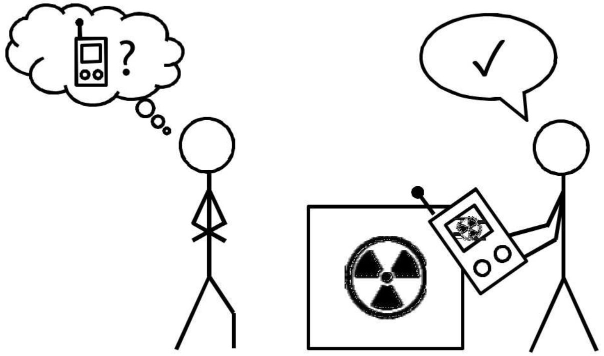
Intro

Hypothetical future arms control treaty verification and monitoring regimes are likely to require trusted technologies to give all parties confidence that treaty obligations are being met



These systems are likely to be subject to authentication and certification requirements, which are defined by the International Partnership for Nuclear Disarmament and Verification (IPNDV) as:

Authentication – A mechanism by which a verification entity obtains confidence that the information reported by monitoring equipment accurately reflects the true state of an item that is subject to verification, and that the monitoring equipment has not been altered, removed or replaced, and functions such that it provides accurate and reproducible results at all times.



Certification – A mechanism by which an inspected State assures itself that an inspection or monitoring system meets safety and security requirements and will not disclose sensitive information (including proliferation-sensitive information) to an inspector

Goals

Trusted system development is time-consuming and costly and typically results in a system tailored for a specific purpose

As an alternative approach we are developing an architecture that enables transparent development of modular components for use in trusted radiation detection systems

Our envisioned architecture will include:

- Module functional requirements
- Module interface specifications
- High-level inspection and testing procedures

Development will be an iterative process

- Define an initial architecture that meets functional requirements while facilitating authentication and certification procedures
- Investigate the perceived benefits of the architecture by developing and testing prototypes of conforming modules
- Revise architecture based on lessons learned in design prototyping and testing

Motivation

Trust is difficult to establish in complex systems

- Microprocessor-based systems with large amounts of embedded software make authentication and certification challenging
- Commercial solutions are becoming increasingly more complex, and often include modern features that make them inconvenient for use in secure facilities

Flexibility and modularity are necessary – allowed measurements and equipment may change during the course of treaty negotiations

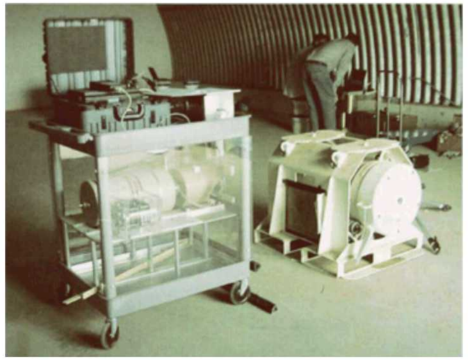
- Enables rapid delivery of a system that will meet negotiated treaty requirements
- Enables the potential to perform multiple types of measurements without having to re-design a full system
- Facilitates functional testing, easing the authentication and certification process

An open architecture would facilitate collaborative design with international treaty partners, which would in turn build trust in the system

- Partners can agree on an architecture and develop conforming modules collaboratively or independently
- Modules from different parties could be interfaced, increasing multi-party trust in the system

Motivating Systems

TRIS – Trusted Radioisotope Identification System
- Designed for gamma spectrum template matching
- Low-resolution scintillator coupled to trusted processor



TRADS – Trusted Radiation Attribute Demonstration System
- Designed for plutonium mass attribute measurements
- High-resolution semiconductor coupled to trusted processor

CONFIDANTE – CONfirmation using a Fast-neutron Imaging Detector with Anti-image Null-positive Time Encoding
- Designed for direct object comparison with neutron imaging
- Pulse-shape discrimination capable scintillator modulated by rotating mask

MC-15
- Designed for neutron multiplicity analysis
- He-3 based system developed for emergency response applications

System Breakdown

System	Active Detector Volume	Signal Conditioning and Pulse Processing	Counting	Acquired Data	Analysis	Output Display
TRIS	Collimated 2”x2” NaI scintillator coupled to a 2” PMT	Shaping preamplifier	N/A	Energy Spectrum	Chi-squared-based comparison to reference spectrum	Confirmation message on user interface
TRADS	High-purity Germanium crtystal	Shaping preamplifier	N/A	Energy spectrum	Minimum mass estimate and Pu-600 algorithm	Confirmation message on user interface
CONFIDANTE	1”x1” Stilbene scintillator coupled to a 2” PMT	Pulse-shape discrimination	Count accumulator for each rotation position	Multiplicity histogram	Feynman multiplicity analysis	Likely a simple confirmation message, but could include the decision metric (actively under development)
MC-15	15 He-3 tubes embedded in a HDPE matrix	Preamplifier and discriminator	Count accumulator for each time window	Multiplicity histogram	Feynman multiplicity analysis	Multiplication and Pu-240 equivalent mass

Design Principles

1. Modules will have simple functionality with well-defined inputs and outputs

   - Restricted functionality of modules motivates simple design and aids in the ability to verify the functionality of a module

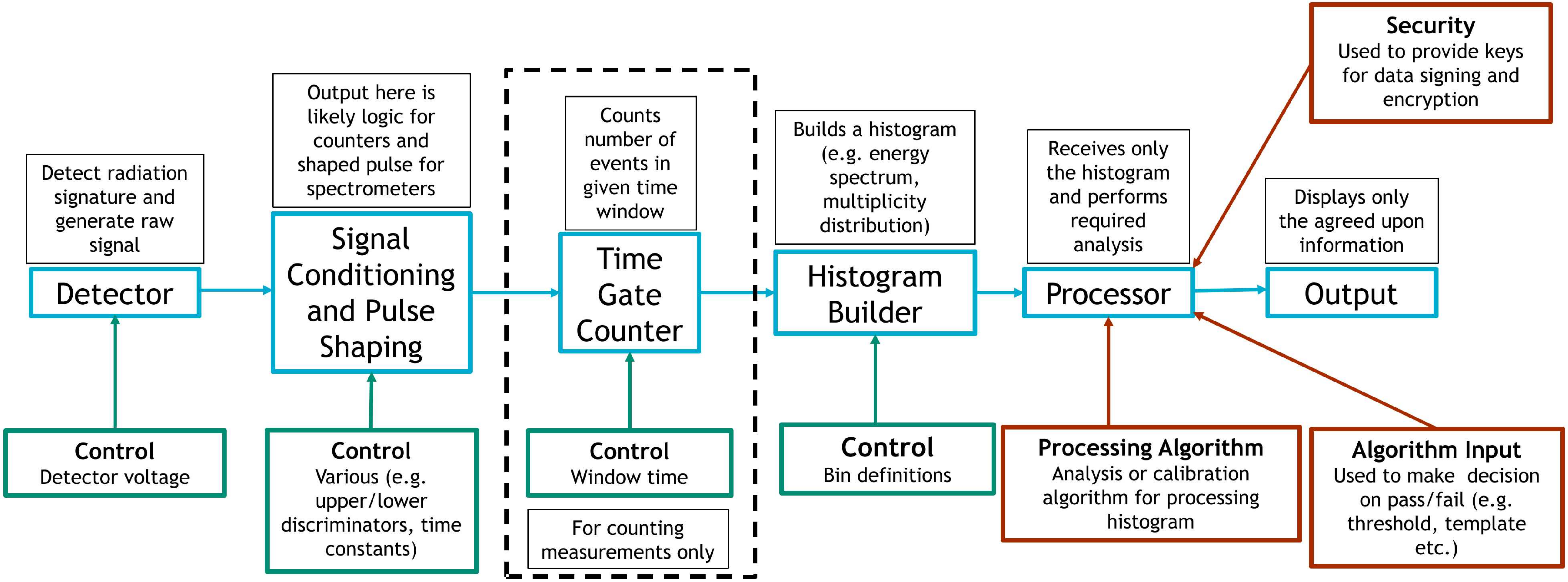
2. Modules will be self-contained – all necessary controls will be on the module and each module can maintain its functionality without communication from other modules

   - Modules can be independently inspected allowing more complex systems to be built without dramatically increasing authentication and certification concerns

3. Data and signals will only flow in one direction through the chain of modules

   - One-way data flow inhibits the ability of “downstream” modules to control “upstream” modules, mitigating some risk associated with hidden switches

A Notional Architecture



Module Functional Requirements

Detector Module

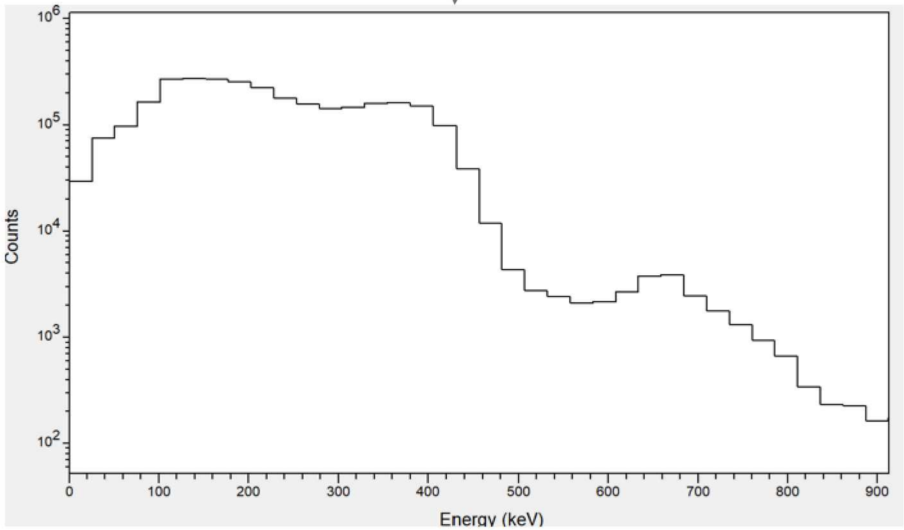
- Detect radiation signature and generate raw signal
- Includes:
  - Detector medium
  - PMT/SiPM (etc.)
  - Any necessary preamplification to bring signal into range of module interface
- Onboard voltage control

Signal Conditioning and Pulse Processing

- Prepares signal for input to Histogram Builder
- Can be a chain of modules between Detector and Histogram Builder modules
- Each module has a specific functionality, and onboard controls to meet that functionality
- Functions might include:
  - Upper/lower level discriminators
  - Pulse shaping
  - Time Gate Counter – converts counts in time window to a proportional voltage pulse for input to Histogram Builder

Histogram Builder Module

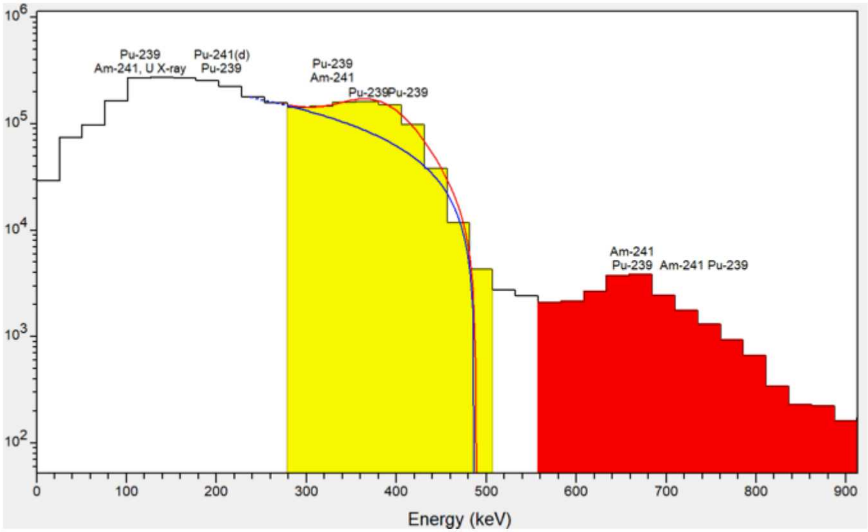
- Convert analog pulses directly to a histogrammed data set (e.g. energy spectrum or multiplicity distribution)
  - Does not digitize the incoming waveform or pickoff exact value of interest (e.g. pulse height)
- Limited channel count
  - Onboard channel edge adjustments – can be set to suit the requirements of the verification system and easily verified in the authentication and certification process
  - Possibility to link several units together to increase channel count
- Accumulates histogram for a fixed time or number of counts
- Histogram is not shared with the Processor module until the measurement is complete



Module Functional Requirements

Processor Module

- Analyzes the histogram to produce a result
- Limited processing power and memory
- Algorithms stored externally – only one instruction set plugged in at a time
- Additional inputs to allow for additional algorithm inputs (e.g. templates, attribute thresholds, etc.) and for any necessary encryption/signing protocols



Output Module

- Display the result determined by the Processor module
- Designed to ensure that only the agreed upon information is released to the observers

Ongoing and Future Efforts

Working towards finalizing initial architecture

- Broad functional requirements have been defined
- Interface specifications and additional input/output requirements are in progress

Developing input/output testing procedures

- Procedures to be defined at module specification level
- Focus on the use of common lab equipment for inspection (e.g. function generators, oscilloscopes, multimeters)

Developing first revision prototype for Histogram Builder Module

- Allows us to explore the concept of limited binning and direct-to-histogram processing
- Current design includes:
  - 16 "on" channels that can be set independently with non-linear spacing
  - "On" channels alternate with "off" channels to allow for non-continuous binning
- By itself this module has the potential to lead to a niche multi-channel analyzer design that facilitates authentication and certification procedures

Future efforts will need to consider tamper indication on the module level and potentially full-system level

Summary and Conclusions

We are developing an architecture to enable transparent development of modular components for use in trusted radiation detection systems

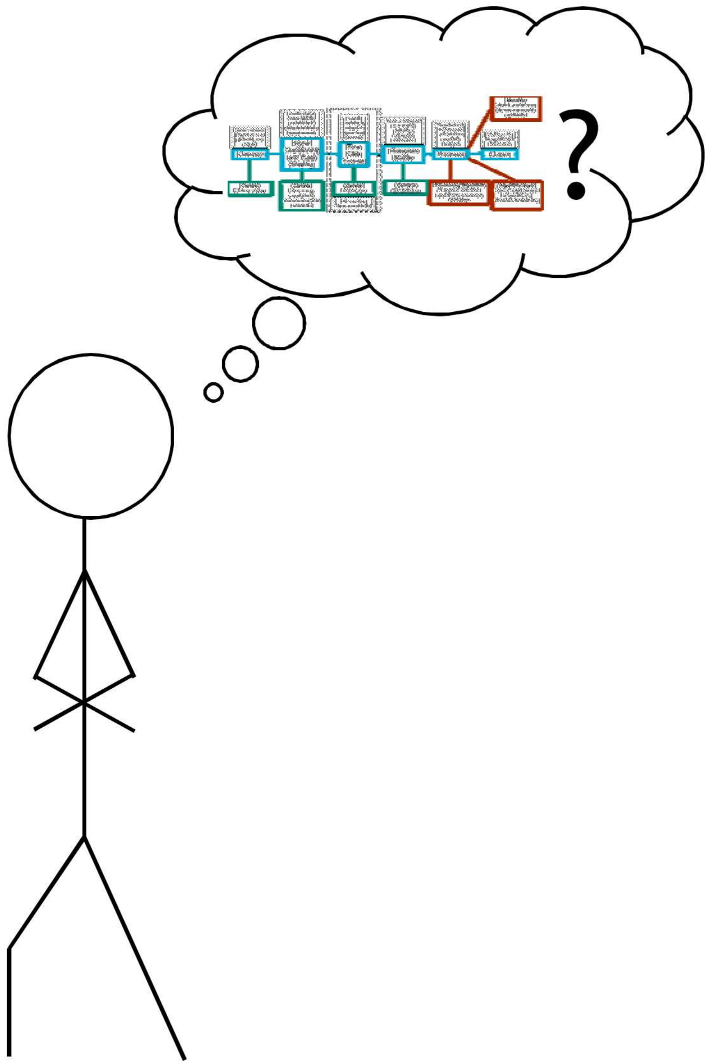
- Novel approach that enables incorporation of critical design features required by treaties while simultaneously increasing the flexibility and facilitating authentication and certification
- A modular architecture is ideal for rapidly assembling, authenticating, and certifying a variety of radiation detection systems for ACTV applications and could reduce costs

To date, we have established a preliminary architecture with several perceived advantages and many open questions that we need to explore

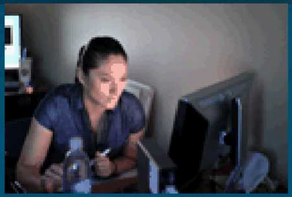
- Should allow for the implementation of a variety of state-of-the-art detection systems
- Provides flexibility to substitute new detectors and/or processing algorithms
- Could potentially support treaty verification activities unrelated to warhead confirmation or even radiation detection

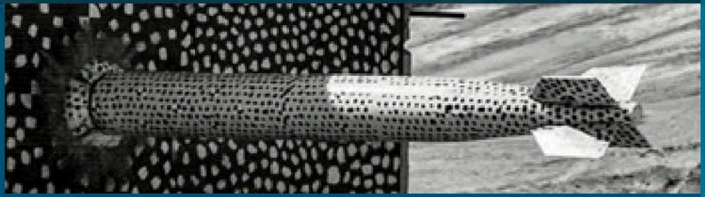
We are currently working to finalize the initial architecture specifications and will design, prototype, and test a selection of conforming modules to understand where improvements can be made

Questions?



A Modular Approach to Trusted System Design for Arms Control Treaty Verification





PRESENTED BY

J. K. Polack, E. Brubaker, M. C. Hamel, R. R. Helguero, D. L. Maierhafer, P. Marleau, E. A. Padilla, T. M. Weber

13 July 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.